DRAFT International Standard

ISO/IEC DIS 5962

Information technology — SPDX® Specification V3.0

Technologies de l'information — Spécification SPDX® V3.0

ICS: 35.080

ISO/IEC JTC **1**

Secretariat: **ANSI**

Voting begins on:
2026-03-16

Voting terminates on:
2026-06-08

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 5962:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Foreword xiii

Introduction xiv

1 Scope 1

2 Normative references 1

3 Symbols 3

4 Terms and definitions 4

5 Conformance 4
5.1 Alternate notation for some conformance requirements 4
5.2 Introduction to profiles 5
5.3 Core profile compliance point 5
5.4 Software profile compliance point 5
5.5 Security profile compliance point 6
5.6 Licensing profile compliance point 6
5.7 Dataset profile compliance point 6
5.8 AI profile compliance point 6
5.9 Build profile compliance point 7
5.10 Lite profile compliance point 7
5.11 Extension profile compliance point 7
5.12 Trademark compliance 8

6 Model and serializations 8
6.1 Overview 8
6.2 RDF serialization 8
6.3 Canonical serialization 9
6.4 Serialization information 9
6.5 Serialization in SPDX 3 JSON 10
6.5.1 A strict subset of JSON-LD 10
6.5.2 JSON-LD context file 10
6.5.3 JSON-LD validation 10

7 Core 10
7.1 Profile information 10
7.1.1 Core profile 10
7.2 Classes 11
7.2.1 Agent 11
7.2.2 Annotation 11
7.2.3 Artifact 12
7.2.4 Bom 14
7.2.5 Bundle 15
7.2.6 CreationInfo 16
7.2.7 DictionaryEntry 16
7.2.8 Element 17
7.2.9 ElementCollection 18
7.2.10 ExternalIdentifier 19
7.2.11 ExternalMap 20
7.2.12 ExternalRef 21
7.2.13 Hash 21
7.2.14 IndividualElement 22
7.2.15 IntegrityMethod 23

© ISO/IEC 2026 – All rights reserved

7.2.16 LifecycleScopedRelationship 24
7.2.17 NamespaceMap 25
7.2.18 Organization 26
7.2.19 PackageVerificationCode 27
7.2.20 Person 28
7.2.21 PositiveIntegerRange 29
7.2.22 Relationship 29
7.2.23 SoftwareAgent 30
7.2.24 SpdxDocument 31
7.2.25 Tool 32
7.3 Properties 33
7.3.1 algorithm 33
7.3.2 annotationType 33
7.3.3 beginIntegerRange 34
7.3.4 builtTime 34
7.3.5 comment 34
7.3.6 completeness 35
7.3.7 contentType 35
7.3.8 context 36
7.3.9 created 36
7.3.10 createdBy 37
7.3.11 createdUsing 37
7.3.12 creationInfo 37
7.3.13 dataLicense 38
7.3.14 definingArtifact 39
7.3.15 description 39
7.3.16 element 39
7.3.17 endIntegerRange 40
7.3.18 endTime 40
7.3.19 extension 41
7.3.20 externalIdentifier 41
7.3.21 externalIdentifierType 41
7.3.22 externalRef 42
7.3.23 externalRefType 42
7.3.24 externalSpdxId 42
7.3.25 from 43
7.3.26 hashValue 43
7.3.27 identifier 44
7.3.28 identifierLocator 44
7.3.29 import 44
7.3.30 issuingAuthority 45
7.3.31 key 45
7.3.32 locationHint 45
7.3.33 locator 46
7.3.34 name 46
7.3.35 namespace 47
7.3.36 namespaceMap 47
7.3.37 originatedBy 47
7.3.38 packageVerificationCodeExcludedFile 48
7.3.39 prefix 48
7.3.40 profileConformance 48
7.3.41 relationshipType 49
7.3.42 releaseTime 49

© ISO/IEC 2026 – All rights reserved

7.3.43 rootElement 50
7.3.44 scope 50
7.3.45 spdxId 50
7.3.46 specVersion 51
7.3.47 standardName 51
7.3.48 startTime 52
7.3.49 statement 52
7.3.50 subject 52
7.3.51 summary 53
7.3.52 suppliedBy 53
7.3.53 supportLevel 54
7.3.54 to 54
7.3.55 validUntilTime 54
7.3.56 value 55
7.3.57 verifiedUsing 55
7.4 Vocabularies 56
7.4.1 AnnotationType 56
7.4.2 ExternalIdentifierType 56
7.4.3 ExternalRefType 57
7.4.4 HashAlgorithm 59
7.4.5 LifecycleScopeType 60
7.4.6 PresenceType 60
7.4.7 ProfileIdentifierType 60
7.4.8 RelationshipCompleteness 61
7.4.9 RelationshipType 62
7.4.10 SupportType 64
7.5 Individuals 65
7.5.1 NoAssertionElement 65
7.5.2 NoneElement 66
7.5.3 SpdxOrganization 66
7.6 Datatypes 66
7.6.1 DateTime 66
7.6.2 MediaType 67
7.6.3 SemVer 67

8 Software 68
8.1 Profile information 68
8.1.1 Software profile 68
8.2 Classes 68
8.2.1 ContentIdentifier 68
8.2.2 File 69
8.2.3 Package 70
8.2.4 Sbom 72
8.2.5 Snippet 73
8.2.6 SoftwareArtifact 74
8.3 Properties 76
8.3.1 additionalPurpose 76
8.3.2 attributionText 76
8.3.3 byteRange 77
8.3.4 contentIdentifier 77
8.3.5 contentIdentifierType 78
8.3.6 contentIdentifierValue 78
8.3.7 copyrightText 78
8.3.8 downloadLocation 79

© ISO/IEC 2026 – All rights reserved

8.3.9 fileKind ... 79
8.3.10 homePage ... 80
8.3.11 lineRange ... 80
8.3.12 packageUrl ... 81
8.3.13 packageVersion ... 81
8.3.14 primaryPurpose ... 82
8.3.15 sbomType ... 82
8.3.16 snippetFromFile ... 82
8.3.17 sourceInfo ... 83
8.4 Vocabularies ... 83
8.4.1 ContentIdentifierType ... 83
8.4.2 FileKindType ... 84
8.4.3 SbomType ... 84
8.4.4 SoftwarePurpose ... 85
9 Security ... 86
9.1 Profile information ... 86
9.1.1 Security profile ... 86
9.2 Classes ... 86
9.2.1 CvssV2VulnAssessmentRelationship ... 86
9.2.2 CvssV3VulnAssessmentRelationship ... 88
9.2.3 CvssV4VulnAssessmentRelationship ... 90
9.2.4 EpssVulnAssessmentRelationship ... 92
9.2.5 ExploitCatalogVulnAssessmentRelationship ... 94
9.2.6 SsvcVulnAssessmentRelationship ... 96
9.2.7 VexAffectedVulnAssessmentRelationship ... 97
9.2.8 VexFixedVulnAssessmentRelationship ... 99
9.2.9 VexNotAffectedVulnAssessmentRelationship ... 100
9.2.10 VexUnderInvestigationVulnAssessmentRelationship ... 102
9.2.11 VexVulnAssessmentRelationship ... 104
9.2.12 VulnAssessmentRelationship ... 105
9.2.13 Vulnerability ... 107
9.3 Properties ... 109
9.3.1 actionStatement ... 109
9.3.2 actionStatementTime ... 109
9.3.3 assessedElement ... 110
9.3.4 catalogType ... 110
9.3.5 decisionType ... 111
9.3.6 exploited ... 111
9.3.7 impactStatement ... 111
9.3.8 impactStatementTime ... 112
9.3.9 justificationType ... 112
9.3.10 locator ... 113
9.3.11 modifiedTime ... 113
9.3.12 percentile ... 113
9.3.13 probability ... 114
9.3.14 publishedTime ... 114
9.3.15 score ... 114
9.3.16 severity ... 115
9.3.17 statusNotes ... 115
9.3.18 vectorString ... 116
9.3.19 vexVersion ... 116
9.3.20 withdrawnTime ... 117
9.4 Vocabularies ... 117

© ISO/IEC 2026 – All rights reserved

9.4.1 CvssSeverityType 117
9.4.2 ExploitCatalogType 118
9.4.3 SsvcDecisionType 118
9.4.4 VexJustificationType 119

10 Licensing 119
10.1 Profile information 119
10.1.1 Licensing profile 119

11 SimpleLicensing 121
11.1 Profile information 121
11.1.1 SimpleLicensing profile 121
11.2 Classes 121
11.2.1 AnyLicenseInfo 121
11.2.2 LicenseExpression 122
11.2.3 SimpleLicensingText 123
11.3 Properties 124
11.3.1 customIdToUri 124
11.3.2 licenseExpression 125
11.3.3 licenseListVersion 125
11.3.4 licenseText 126

12 ExpandedLicensing 126
12.1 Profile information 126
12.1.1 ExpandedLicensing profile 126
12.2 Classes 127
12.2.1 ConjunctiveLicenseSet 127
12.2.2 CustomLicense 128
12.2.3 CustomLicenseAddition 129
12.2.4 DisjunctiveLicenseSet 130
12.2.5 ExtendableLicense 131
12.2.6 IndividualLicensingInfo 131
12.2.7 License 132
12.2.8 LicenseAddition 133
12.2.9 ListedLicense 135
12.2.10 ListedLicenseException 136
12.2.11 OrLaterOperator 137
12.2.12 WithAdditionOperator 138
12.3 Properties 139
12.3.1 additionText 139
12.3.2 deprecatedVersion 139
12.3.3 isDeprecatedAdditionId 140
12.3.4 isDeprecatedLicenseId 140
12.3.5 isFsfLibre 141
12.3.6 isOsiApproved 141
12.3.7 licenseXml 142
12.3.8 listVersionAdded 142
12.3.9 member 143
12.3.10 obsoletedBy 143
12.3.11 seeAlso 144
12.3.12 standardAdditionTemplate 144
12.3.13 standardLicenseHeader 145
12.3.14 standardLicenseTemplate 145
12.3.15 subjectAddition 145
12.3.16 subjectExtendableLicense 146

© ISO/IEC 2026 – All rights reserved

12.3.17 subjectLicense 146
12.4 Individuals 147
12.4.1 NoAssertionLicense 147
12.4.2 NoneLicense 147

13 Dataset 147
13.1 Profile information 147
13.1.1 Dataset profile 147
13.2 Classes 148
13.2.1 DatasetPackage 148
13.3 Properties 150
13.3.1 anonymizationMethodUsed 150
13.3.2 confidentialityLevel 150
13.3.3 dataCollectionProcess 151
13.3.4 dataPreprocessing 151
13.3.5 datasetAvailability 152
13.3.6 datasetNoise 152
13.3.7 datasetSize 152
13.3.8 datasetType 153
13.3.9 datasetUpdateMechanism 153
13.3.10 hasSensitivePersonalInformation 154
13.3.11 intendedUse 154
13.3.12 knownBias 154
13.3.13 sensor 155
13.4 Vocabularies 155
13.4.1 ConfidentialityLevelType 155
13.4.2 DatasetAvailabilityType 156
13.4.3 DatasetType 156

14 AI 157
14.1 Profile information 157
14.1.1 AI profile 157
14.1.2 Profile conformance 157
14.2 Classes 157
14.2.1 AIPackage 157
14.2.2 EnergyConsumption 160
14.2.3 EnergyConsumptionDescription 161
14.3 Properties 162
14.3.1 autonomyType 162
14.3.2 domain 162
14.3.3 energyConsumption 162
14.3.4 energyQuantity 163
14.3.5 energyUnit 163
14.3.6 finetuningEnergyConsumption 164
14.3.7 hyperparameter 164
14.3.8 inferenceEnergyConsumption 164
14.3.9 informationAboutApplication 165
14.3.10 informationAboutTraining 165
14.3.11 limitation 166
14.3.12 metric 166
14.3.13 metricDecisionThreshold 167
14.3.14 modelDataPreprocessing 167
14.3.15 modelExplainability 168
14.3.16 safetyRiskAssessment 168

© ISO/IEC 2026 – All rights reserved

14.3.17 standardCompliance....169
14.3.18 trainingEnergyConsumption....169
14.3.19 typeOfModel....169
14.3.20 useSensitivePersonalInformation....170
14.4 Vocabularies....170
14.4.1 EnergyUnitType....170
14.4.2 SafetyRiskAssessmentType....171
15 Build....171
15.1 Profile information....171
15.1.1 Build profile....171
15.2 Classes....172
15.2.1 Build....172
15.3 Properties....173
15.3.1 buildEndTime....173
15.3.2 buildId....174
15.3.3 buildStartTime....174
15.3.4 buildType....175
15.3.5 configSourceDigest....175
15.3.6 configSourceEntrypoint....176
15.3.7 configSourceUri....176
15.3.8 environment....177
15.3.9 parameter....177
16 Lite....178
16.1 Profile information....178
16.1.1 Lite profile....178
17 Extension....179
17.1 Profile information....179
17.1.1 Extension profile....179
17.2 Classes....179
17.2.1 CdxPropertiesExtension....179
17.2.2 CdxPropertyEntry....180
17.2.3 Extension....180
17.3 Properties....181
17.3.1 cdxPropName....181
17.3.2 cdxPropValue....182
17.3.3 cdxProperty....182
Annex A (informative) RDF model definition and diagrams....183
A.1 Model definition....183
A.2 Diagrams....183
A.2.1 Core profile....183
A.2.2 Software profile....184
A.2.3 Security profile....185
A.2.4 Licensing profile....186
A.2.5 Dataset profile....187
A.2.6 AI profile....188
A.2.7 Build profile....189
A.2.8 Extension profile....190

© ISO/IEC 2026 – All rights reserved

Annex B (normative) SPDX license expressions **191**
B.1 Overview **191**
B.2 Case sensitivity **192**
B.3 Simple license expressions **192**
B.4 Composite license expressions **192**
B.4.1 Introduction **192**
B.4.2 Disjunctive "OR" operator **192**
B.4.3 Conjunctive "AND" operator **193**
B.4.4 Additive "WITH" operator **193**
B.4.5 Order of precedence and parentheses **193**
B.5 Complete grammar **194**
Annex C (normative) SPDX License List matching guidelines and templates **195**
C.1 SPDX License List matching guidelines **195**
C.2 How these guidelines are applied **195**
C.2.1 Purpose **195**
C.2.2 Guideline: official license headers **195**
C.3 Substantive text **195**
C.3.1 Purpose **195**
C.3.2 Guideline: verbatim text **195**
C.3.3 Guideline: no additional text **195**
C.3.4 Guideline: replaceable text **195**
C.3.5 Guideline: omittable text **196**
C.4 Whitespace **196**
C.4.1 Purpose **196**
C.4.2 Guideline **196**
C.5 Capitalization **196**
C.5.1 Purpose **196**
C.5.2 Guideline **196**
C.6 Punctuation **197**
C.6.1 Purpose **197**
C.6.2 Guideline: punctuation **197**
C.6.3 Guideline: hyphens, dashes **197**
C.6.4 Guideline: quotes **197**
C.7 Code comment indicators or separators **197**
C.7.1 Purpose **197**
C.7.2 Guideline: prefix **197**
C.7.3 Guideline: repeated characters **197**

© ISO/IEC 2026 – All rights reserved

C.8 Bullets and numbering 197
C.8.1 Purpose 197
C.8.2 Guideline 197
C.9 Varietal word spelling 198
C.9.1 Purpose 198
C.9.2 Guideline 198
C.10 Copyright symbol 198
C.10.1 Purpose 198
C.10.2 Guideline 198
C.11 Copyright notice 198
C.11.1 Purpose 198
C.11.2 Guideline 198
C.12 License name or title 198
C.12.1 Purpose 198
C.12.2 Guideline 199
C.13 Extraneous text at the end of a license 199
C.13.1 Purpose 199
C.13.2 Guideline 199
C.14 HTTP protocol 199
C.14.1 Purpose 199
C.14.2 Guideline 199
C.15 SPDX License List 199
C.15.1 Template access 199
C.15.2 License List XML format 199
C.15.3 Legacy Text Template format 199
Annex D (normative) SPDX Lite 201
D.1 Explanation of the Lite profile 201
D.2 Mandatory and recommended properties 201
D.2.1 /Core/SpdxDocument 201
D.2.2 /Software/Sbom 201
D.2.3 /Software/Package 202
D.2.4 /Core/Hash 202
D.2.5 /SimpleLicensing/LicenseExpression 203
D.2.6 /SimpleLicensing/SimpleLicensingText 203
D.2.7 /Core/Agent (createdBy, suppliedBy, originatedBy) 203
D.2.8 /Core/CreationInfo 203
D.2.9 /Core/ExternalIdentifier 203

© ISO/IEC 2026 – All rights reserved

D.2.10 /Core/NameSpaceMap 204
D.2.11 /Core/Relationship 204
Annex E (normative) Package URL specification v1 205
E.1 Introduction 205
E.2 Syntax definition 205
E.3 Character encoding 206
E.4 Rules for each component 206
E.4.1 Rules for scheme 206
E.4.2 Rules for type 207
E.4.3 Rules for namespace 207
E.4.4 Rules for name 207
E.4.5 Rules for version 207
E.4.6 Rules for qualifiers 207
E.4.7 Rules for subpath 208
E.5 Known types 208
E.6 Known qualifiers key/value pairs 208
E.7 How to produce and consume *purl* data 208
E.7.1 How to build *purl* string from its components 208
E.7.2 How to parse a *purl* string to its components 210
E.8 Examples 211
E.9 Original license 211

© ISO/IEC 2026 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by The Linux Foundation and its Contributors under the SPDX Working Group (as SPDX® Specification v3.0) and drafted in accordance with its editorial rules. Its preparation and publication has been made in coordination with related efforts with the Object Management Group (OMG). It was adopted, under the JTC 1 PAS ("Publicly Available Specification") procedure, by Joint Technical Committee ISO/IEC JTC 1, Information technology.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

This specification replaces ISO/IEC 5962:2021, which described SPDX version 2.2.1.

© ISO/IEC 2026 – All rights reserved

Introduction

Companies and organizations (collectively “Organizations”) are widely using and reusing open source and other software packages. Accurate identification of software is key for many supply chain processes. Vulnerability remediation starts with knowing the details of which version of software is in use on a system. Compliance with the associated licenses requires a set of analysis activities and due diligence that each Organization performs independently, which may include a manual and/or automated scan of software and identification of associated licenses followed by manual verification.

Software development teams across the globe use the same open source packages, but little infrastructure exists to facilitate collaboration on the analysis or share the results of these analysis activities. As a result, many groups are performing the same work leading to duplicated efforts and redundant information. With this document, the SPDX workgroup, a combined effort of the Linux Foundation SPDX group and the OMG/CISQ Tool-to-Tool effort, has created a data exchange format so that information about software packages and related content may be collected and shared in a common format with the goal of saving time and improving data accuracy.

The merged activities of the two groups slid together the beginning weeks of 2021 with activities generally moving forward but occasionally stalling while the larger group worked through issues that one or the other hadn’t discussed or had a different opinion about. Eventually, after releasing SPDX 2.3 in August of 2022 with updates that brought some of the concepts and capabilities slated for SPDX 3.0 to the community in preparation of the shift that SPDX 3.0 represents, the first release candidate of SPDX 3.0 was released in May of 2023. Within the SPDX community, which is both a standards creation organization as well as a community of open source developers, a release candidate offers an opportunity for implementors of SPDX, both new and old, to review the work and determine whether there were parts that were unclear or that would be extremely burdensome to implement.

Based on the comments and change requests from the initial candidate release several areas of the model were revised and reworked, resulting in a release candidate 2 of SPDX 3.0 in February of 2024. That release candidate gave tool creators and those who maintain the support libraries for working with SPDX time to start revising their projects in advance of the final version of the SPDX 3.0 specification. For those not following the inner workings, debates, and discussion of the combined 3T-SBOM and SPDX 3.0 working group for the last 3 years there has been a dramatic change in the SPDX model as it goes from SPDX 2.3 to SPDX 3.0, shifting the SPDX name from Software Package Data Exchange to System Package Data Exchange and expanding the scope of items it can now convey in a bill of materials from software, security, and licensing to many additional aspects like data sets, AI models, and build information.

Since the release of 3.0.0, the groups have gathered feedback on the level of documentation and minor errors in the model which have been addressed in the 3.0.1 release.

© ISO/IEC 2026 – All rights reserved

Information Technology — SPDX® Specification V3.0

1 Scope

The System Package Data Exchange™ (SPDX®) specification defines an open standard for communicating bill of materials (BOM) information for different topic areas.

SPDX defines an underlying data model as well as multiple serialization formats to encode that data model.

SPDX metadata includes details about creation and distribution, including the following:

- software composition, for collections of software (Packages), individual Files, and portions of files (Snippets)
- software build information
- artificial intelligence (AI) models
- datasets
- creator, supplier and distributor identity information
- provenance and integrity
- licenses and copyrights, including a curated list of licenses and exceptions
- security vulnerabilities, defects, and other quality data
- relationships between system elements
- software usage and lifecycle
- mechanisms to enable annotating SPDX elements and linking between multiple SPDX Documents

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

Apache Maven, Apache Software Foundation, https://maven.apache.org/.

Bower API, https://bower.io/docs/api/#install.

Common Platform Enumeration (CPE) – Specification 2.2, The MITRE Corporation, https://cpe.mitre.org/files/cpe-specification_2.2.pdf.

Common Platform Enumeration (CPE): Naming Specification Version 2.3, NIST IR 7695, NIST, https://csrc.nist.gov/pubs/ir/7695/final.

Common Vulnerability Scoring System v3.0 (CVSS v3.0): Specification Document, Forum of Incident Response and Security Teams, Inc (FIRST), https://www.first.org/cvss/v3.0/specification-document.

Common Vulnerability Scoring System v3.1 (CVSS v3.1): Specification Document, Forum of Incident Response and Security Teams, Inc (FIRST), https://www.first.org/cvss/v3.1/specification-document.

Common Vulnerability Scoring System version 4.0 (CVSS v4.0): Specification Document, Forum of Incident Response and Security Teams, Inc (FIRST), https://www.first.org/cvss/v4.0/specification-document.

CVSS 3.0 schema, Forum of Incident Response and Security Teams, Inc (FIRST), https://www.first.org/cvss/cvss-v3.0.json.

© ISO/IEC 2026 – All rights reserved

CVSS 3.1 schema, Forum of Incident Response and Security Teams, Inc (FIRST), https://www.first.org/cvss/cvss-v3.1.json.

CVSS 4.0 schema, Forum of Incident Response and Security Teams, Inc (FIRST), https://www.first.org/cvss/cvss-v4.0.json.

EU general risk assessment methodology, European Commission, https://ec.europa.eu/docsroom/documents/17107.

npm-package.json, npm Inc., https://docs.npmjs.com/files/package.json.

NuGet documentation, Microsoft, https://docs.nuget.org/.

POSIX.1-2017 *The Open Group Base Specifications Issue 7*, 2018 edition, IEEE/Open Group, https://pubs.opengroup.org/onlinepubs/9699919799/.

Resource Description Framework (RDF), 2014-02-25, W3C, http://www.w3.org/standards/techs/rdf.

RFC 1319, *The MD2 Message-Digest Algorithm*, Internet Engineering Task Force, https://datatracker.ietf.org/doc/rfc1319/.

RFC 1320, *The MD4 Message-Digest Algorithm*, Internet Engineering Task Force, https://datatracker.ietf.org/doc/rfc1320/.

RFC 1321, *The MD5 Message-Digest Algorithm*, Internet Engineering Task Force, https://datatracker.ietf.org/doc/rfc1321/.

RFC 1950, *ZLIB Compressed Data Format Specification version 3.3*, Internet Engineering Task Force, https://datatracker.ietf.org/doc/rfc1950/.

RFC 2046, *Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types*, Internet Engineering Task Force, https://datatracker.ietf.org/doc/rfc2046/.

RFC 3174, *US Secure Hash Algorithm 1 (SHA1)*, Internet Engineering Task Force, https://datatracker.ietf.org/doc/rfc3174/.

RFC 3696, *Application Techniques for Checking and Transformation of Names*, Internet Engineering Task Force, https://datatracker.ietf.org/doc/rfc3696/.

RFC 3874, *A 224-bit One-way Hash Function: SHA-224*, Internet Engineering Task Force, https://datatracker.ietf.org/doc/rfc3874/.

RFC 3986, *Uniform Resource Identifier (URI): Generic Syntax*, Internet Engineering Task Force, https://datatracker.ietf.org/doc/rfc3986/.

RFC 5234, *Augmented BNF for Syntax Specifications: ABNF*, Internet Engineering Task Force, https://datatracker.ietf.org/doc/rfc5234/.

RFC 6234, *US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)*, Internet Engineering Task Force, https://datatracker.ietf.org/doc/rfc6234/.

RFC 7405, *Case-Sensitive String Support in ABNF*, Internet Engineering Task Force, https://datatracker.ietf.org/doc/rfc7405/.

RFC 7693, *The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC)*, Internet Engineering Task Force, https://datatracker.ietf.org/doc/rfc7693/.

RFC 8259, *The JavaScript Object Notation (JSON) Data Interchange Format*, Internet Engineering Task Force, https://datatracker.ietf.org/doc/rfc8259/.

RFC 9393, *Concise Software Identification Tags*, Internet Engineering Task Force, https://datatracker.ietf.org/doc/rfc9393/.

Semantic Versioning 2.0.0, Tom Preston-Werner and SemVer contributors, https://semver.org.

© ISO/IEC 2026 – All rights reserved

SLSA Provenance v0.2, The Linux Foundation, https://slsa.dev/spec/v0.2/provenance.

SoftWare Heritage persistent IDentifiers (SWHIDs), in International Standard *ISO/IEC 18670 Information technology — SoftWare Hash IDentifier (SWHID) Specification V1.2*https://www.iso.org/standard/89985.html, also available at https://www.swhid.org/swhid-specification/v1.2/

SPDX and RDF Ontology, http://spdx.org/rdf/ontology/spdx-3-0

SPDX License List, The Linux Foundation, https://spdx.org/licenses/

SPDX License Exceptions, The Linux Foundation, https://spdx.org/licenses/exceptions-index.html

Stakeholder-Specific Vulnerability Categorization Guide, CISA, https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc.

The EPSS Model, Forum of Incident Response and Security Teams, Inc (FIRST), https://www.first.org/epss/model.

Types of Software Bill of Material (SBOM) Documents, CISA, https://www.cisa.gov/sites/default/files/2023-04/sbom-types-document-508c.pdf.

3 Symbols

The following symbols and abbreviations are used throughout this document:

3T-SBOM	Tool-to-Tool Software Bill of Materials Exchange
ABNF	Augmented Backus–Naur form
AI	Artificial Intelligence
BNF	Backus–Naur form
BOM	Bill of Materials
CISA	Cybersecurity and Infrastructure Security Agency
CISQ	Consortium for Information & Software Quality
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
EPSS	Exploit Prediction Scoring System
ISO	International Organization for Standardization
JSON-LD	JavaScript Object Notation for Linking Data
KEV	Known Exploited Vulnerabilities
ML	Machine Learning
NIST	National Institute of Standards and Technology
NISTIR	NIST Internal or Interagency Report
NTIA	National Telecommunications and Information Administration
OSI	Open Source Initiative
OWL	Web Ontology Language
PAS	Publicly Available Specification

© ISO/IEC 2026 – All rights reserved

POSIX	Portable Operating System Interface
PTF	Platform Task Force
PURL	Package URL
RDF	Resource Description Framework
RFC	Request For Comments
SBOM	Software Bill of Materials
SHA	Secure Hash Algorithms
SHACL	Shapes Constraint Language
SPDX	System Package Data Exchange (previously Software Package Data Exchange)
SSVC	Stakeholder-Specific Vulnerability Categorization
SWHID	SoftWare Hash IDentifier
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VEX	Vulnerability Exploitability eXchange
XML	Extensible Markup Language

4 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at http://www.electropedia.org/

4.1
profile
a scope of usage for SPDX targeting support for particular use cases and scenarios (e.g., software, licensing, security, etc.) that identifies which particular SPDX namespaces, classes, and properties it leverages, along with any custom constraints unique to its use

5 Conformance

5.1 Alternate notation for some conformance requirements

This document contains more than a few cardinality assertions, each of which indicates the minimum and maximum number of times a property may appear. These are represented by using “minCount” and “maxCount” respectively. The absolute minimum number of occurrences is zero (0), while for an unbounded maximum number of occurrences a star (*) is being used.

Here are some examples:

- minCount: 1
- maxCount: *
- Cardinality: 0..1
- Cardinality: 0..*

© ISO/IEC 2026 – All rights reserved